SPYWOLF

Security Audit Report

Completed on
January 2, 2023

SPYWOLF.CO
@SPYWOLFNETWORK
@SPYWOLFNETWORK

OVERVIEW

This audit has been prepared for **Bubble DeFi** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

> *The results of this audit are purely based on the team’s evaluation and does not guarantee nor reflect the projects outcome and goal*
>
> - SPYWOLF Team -

TABLE OF CONTENTS

BUBBLE DEFI

PROJECT DESCRIPTION

According to their whitepaper:
Bubble DeFi is a decentralized ecosystem creating sustainable liquidity products for decentralized finance (DeFi). The protocol allows users to create their own liquid assets and provides a marketplace for buying/selling them.

Release Date: Presale starts in January, 2023

Category: DeFi

CONTRACT 1 INFO

Token Name
Bubble

Symbol
BUB

Contract Address
0x0b191f0F202033E22467d967d970048aa22AcB2a

Network
Ethereum

Language
Solidity

Deployment Date
Jan 1, 2023

Verified?
Yes

Total Supply
100,000,000

Status
Not launched

TAXES

Buy Tax
5%

Sell Tax
5%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

CURRENT STATS

(As of January 2, 2023)

Liquidity

Not added yet

Burn

No burnt tokens

Status:

Not Launched!

MaxTxAmount
2,000,000

DEX
Uniswap

LP Address(es)

Liquidity not added yet

TOKEN TRANSFERS STATS

Transfer Count	1
Uniq Senders	1
Uniq Receivers	1
Total Amount	100000000 BUB
Median Transfer Amount	100000000 BUB
Average Transfer Amount	100000000 BUB
First transfer date	2023-01-01
Last transfer date	2023-01-01
Days token transferred	1

SMART CONTRACT STATS

Calls Count	1
External calls	1
Internal calls	0
Transactions count	1
Uniq Callers	1
Days contract called	1
Last transaction time	2023-01-01 19:02:47 UTC
Created	2023-01-01 19:02:47 UTC
Create TX	0x84156a7f5d86f366cf04a8fb1f4bdaf13da7f86b8ed3628e71a96efa1eb7d9d5
Creator	0x1c1197a1d3c93feb06bb9b5000bebe70f4fc440b

FEATURED WALLETS

Owner address	0x1C1197A1d3c93fEb06bB9B5000BEbe70f4fC440B
LP wallet	0x0000000000000000000000000000000000000adD
LP address	**Liquidity not added yet**

TOP 3 UNLOCKED WALLETS

1	100%	Same as owner

Tokens are not distributed yet

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

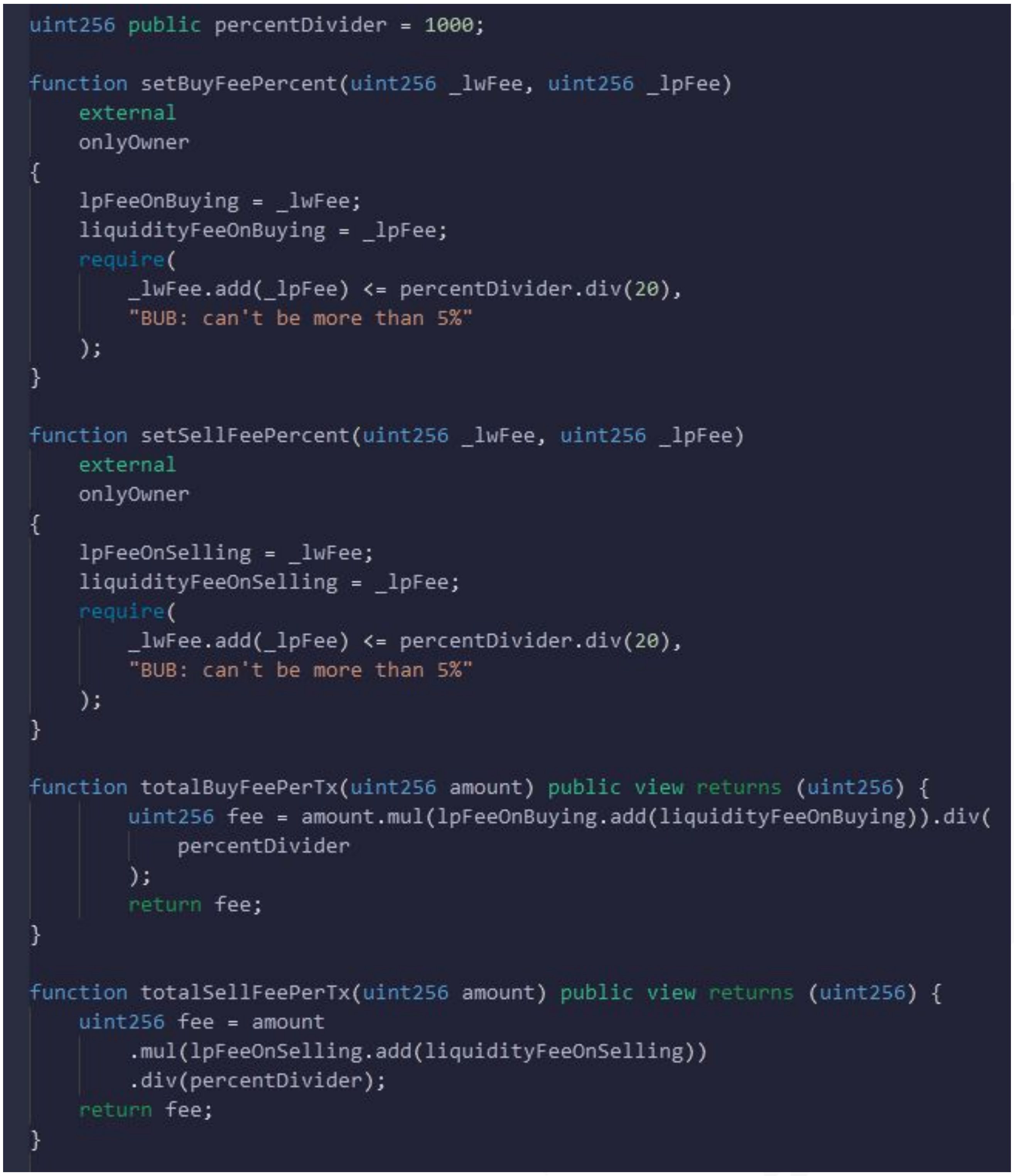
Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

Informational

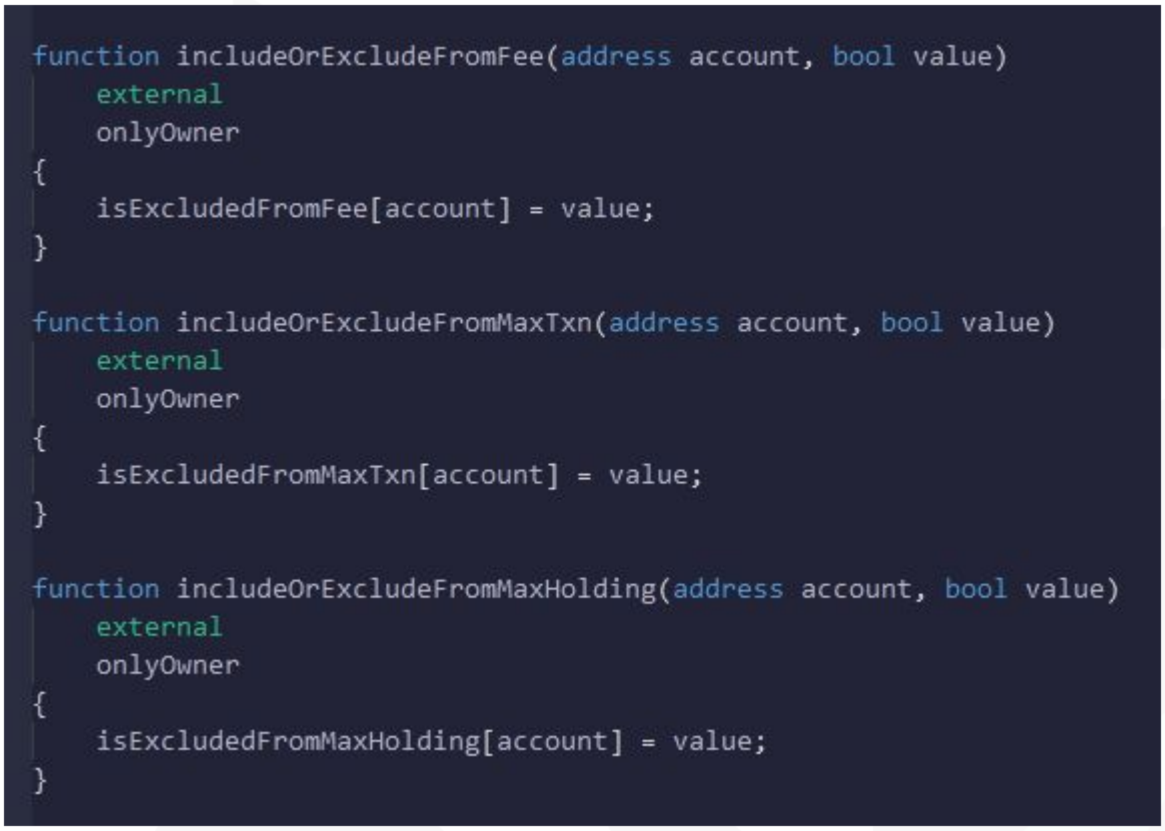
Owner can set buy/sell fees up to 5%.
Combined buy+sell=10%.



```
uint256 public percentDivider = 1000;

function setBuyFeePercent(uint256 _lwFee, uint256 _lpFee)
    external
    onlyOwner
{
    lpFeeOnBuying = _lwFee;
    liquidityFeeOnBuying = _lpFee;
    require(
        _lwFee.add(_lpFee) <= percentDivider.div(20),
        "BUB: can't be more than 5%"
    );
}

function setSellFeePercent(uint256 _lwFee, uint256 _lpFee)
    external
    onlyOwner
{
    lpFeeOnSelling = _lwFee;
    liquidityFeeOnSelling = _lpFee;
    require(
        _lwFee.add(_lpFee) <= percentDivider.div(20),
        "BUB: can't be more than 5%"
    );
}

function totalBuyFeePerTx(uint256 amount) public view returns (uint256) {
        uint256 fee = amount.mul(lpFeeOnBuying.add(liquidityFeeOnBuying)).div(
            percentDivider
        );
        return fee;
}

function totalSellFeePerTx(uint256 amount) public view returns (uint256) {
    uint256 fee = amount
        .mul(lpFeeOnSelling.add(liquidityFeeOnSelling))
        .div(percentDivider);
    return fee;
}
```

Informational

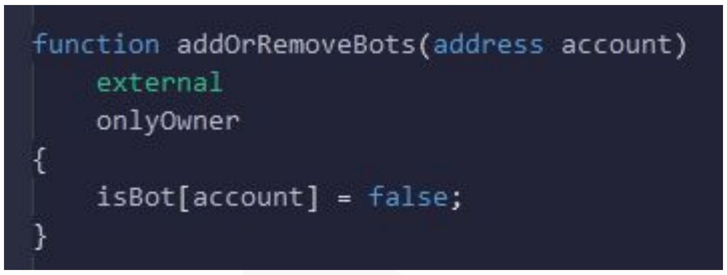
Owner can include/exclude address from fees, max transaction limit and max wallet limit.
If dex pair address is included in max wallet and max wallet limit is too low, selling will fail.



```
function includeOrExcludeFromFee(address account, bool value)
    external
    onlyOwner
{
    isExcludedFromFee[account] = value;
}

function includeOrExcludeFromMaxTxn(address account, bool value)
    external
    onlyOwner
{
    isExcludedFromMaxTxn[account] = value;
}

function includeOrExcludeFromMaxHolding(address account, bool value)
    external
    onlyOwner
{
    isExcludedFromMaxHolding[account] = value;
}
```

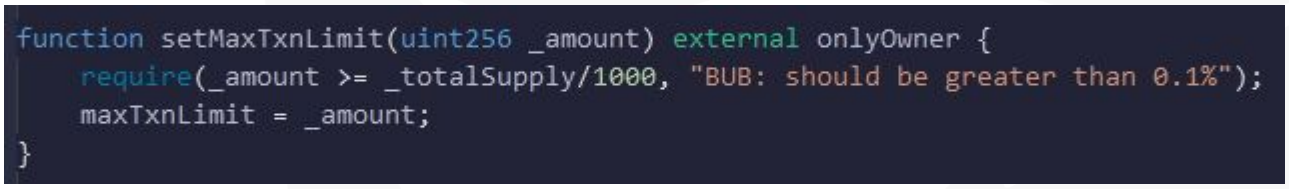
Informational

Owner can only exclude address from blacklist.



```
function addOrRemoveBots(address account)
    external
    onlyOwner
{
    isBot[account] = false;
}
```

Owner can set max transaction limit but cannot lower it than 0.1% of total supply.



```
function setMaxTxnLimit(uint256 _amount) external onlyOwner {
    require(_amount >= _totalSupply/1000, "BUB: should be greater than 0.1%");
    maxTxnLimit = _amount;
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

BUBBLE DEFI (1)

GOOD PRACTICES FOUND

- ✓ The owner cannot mint new tokens after deployment
- ✓ The owner can set max transaction limit, but cannot lower it than 0.1% of total supply.
- ✓ The smart contract utilizes "SafeMath" to prevent overflows

CONTRACT 2 INFO

Token Name
PresaleBub

Symbol
N/A

Contract Address
0x67dA9948a0A5DE7161a8A0B9Dc1523978eB891Fd

Network
Ethereum

Language
Solidity

Deployment Date
January 1, 2023

Verified?
Yes

Total Supply
N/A

Status
Deployed

TAXES

Buy Tax
none

Sell Tax
none

Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

FEATURED WALLETS

Owner address	0x1C1197A1d3c93fEb06bB9B5000BEbe70f4fC440B
LP address	**Presale contract**

TOP 3 UNLOCKED WALLETS

1	N/A	N/A
2	N/A	N/A
3	N/A	N/A

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

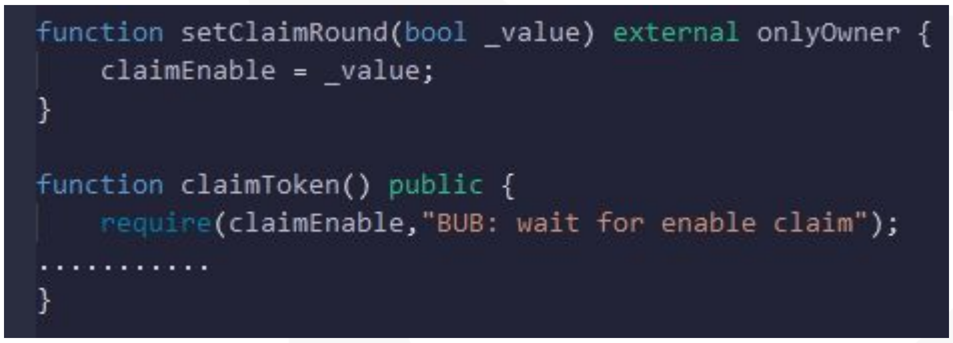
Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ Medium Risk

Owner can enable/disable tokens claim status, making it impossible to claim bought tokens.

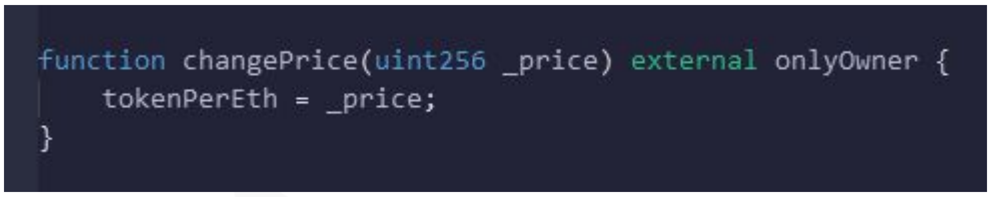


```
function setClaimRound(bool _value) external onlyOwner {
    claimEnable = _value;
}

function claimToken() public {
    require(claimEnable,"BUB: wait for enable claim");
...........
}
```

Explanation from the project developers:
"It's a feature we added in the smart contract that allows for the ability to turn on and off the claim status of the token for improved security of the smart contract. This feature can be used to control the distribution of the tokens to reduce the risk of unauthorized claims if anything goes wrong."

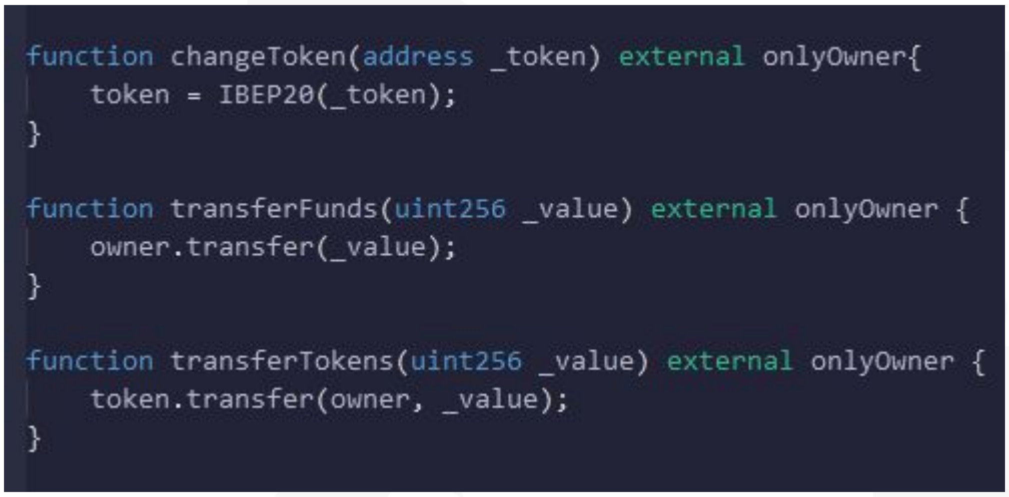
Informational

Owner can change presale tokens price.



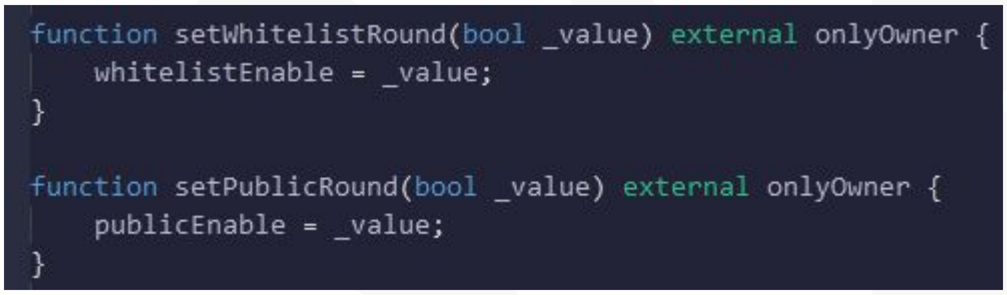
```
function changePrice(uint256 _price) external onlyOwner {
    tokenPerEth = _price;
}
```

Owner can withdraw any tokens from the contract.



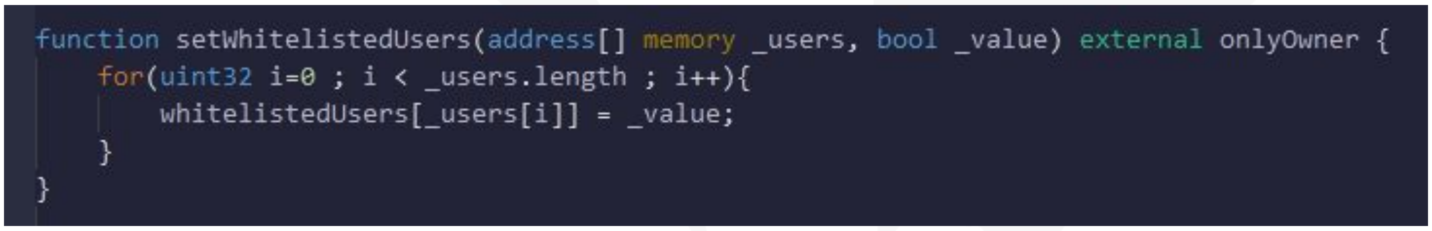
```
function changeToken(address _token) external onlyOwner{
    token = IBEP20(_token);
}

function transferFunds(uint256 _value) external onlyOwner {
    owner.transfer(_value);
}

function transferTokens(uint256 _value) external onlyOwner {
    token.transfer(owner, _value);
}
```

Owner can change presale status to whitelisted/public at any time.



```
function setWhitelistRound(bool _value) external onlyOwner {
    whitelistEnable = _value;
}

function setPublicRound(bool _value) external onlyOwner {
    publicEnable = _value;
}
```

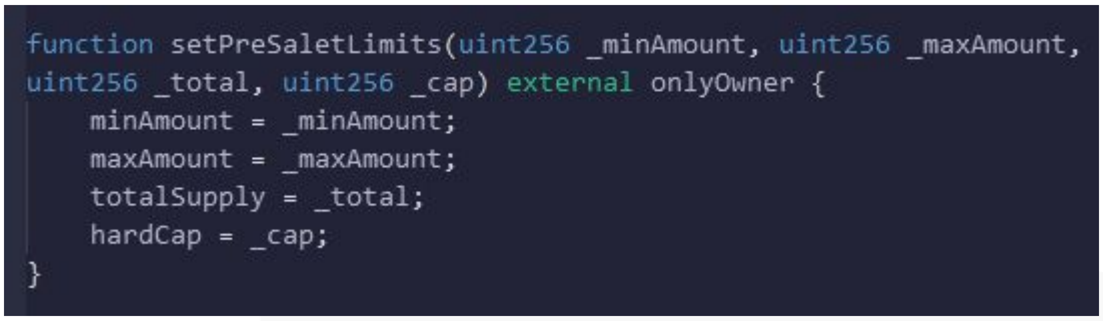
Owner can add any address to whitelist.



```
function setWhitelistedUsers(address[] memory _users, bool _value) external onlyOwner {
    for(uint32 i=0 ; i < _users.length ; i++){
        whitelistedUsers[_users[i]] = _value;
    }
}
```

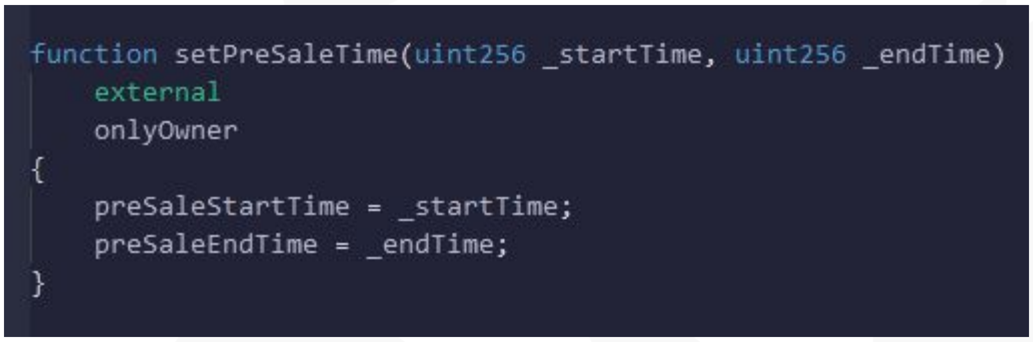
Informational

Owner can change presale settings - min buy amount, max buy amount, hard cap, total presale supply (totalSupply is for informational purpose only).



```
function setPreSaletLimits(uint256 _minAmount, uint256 _maxAmount,
uint256 _total, uint256 _cap) external onlyOwner {
    minAmount = _minAmount;
    maxAmount = _maxAmount;
    totalSupply = _total;
    hardCap = _cap;
}
```

Owner can set presale start/end time at any moment without limitations.



```
function setPreSaleTime(uint256 _startTime, uint256 _endTime)
    external
    onlyOwner
{
    preSaleStartTime = _startTime;
    preSaleEndTime = _endTime;
}
```

If owner's account is out of $BUB tokens, presalers cannot claim their tokens.

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

PresaleBub

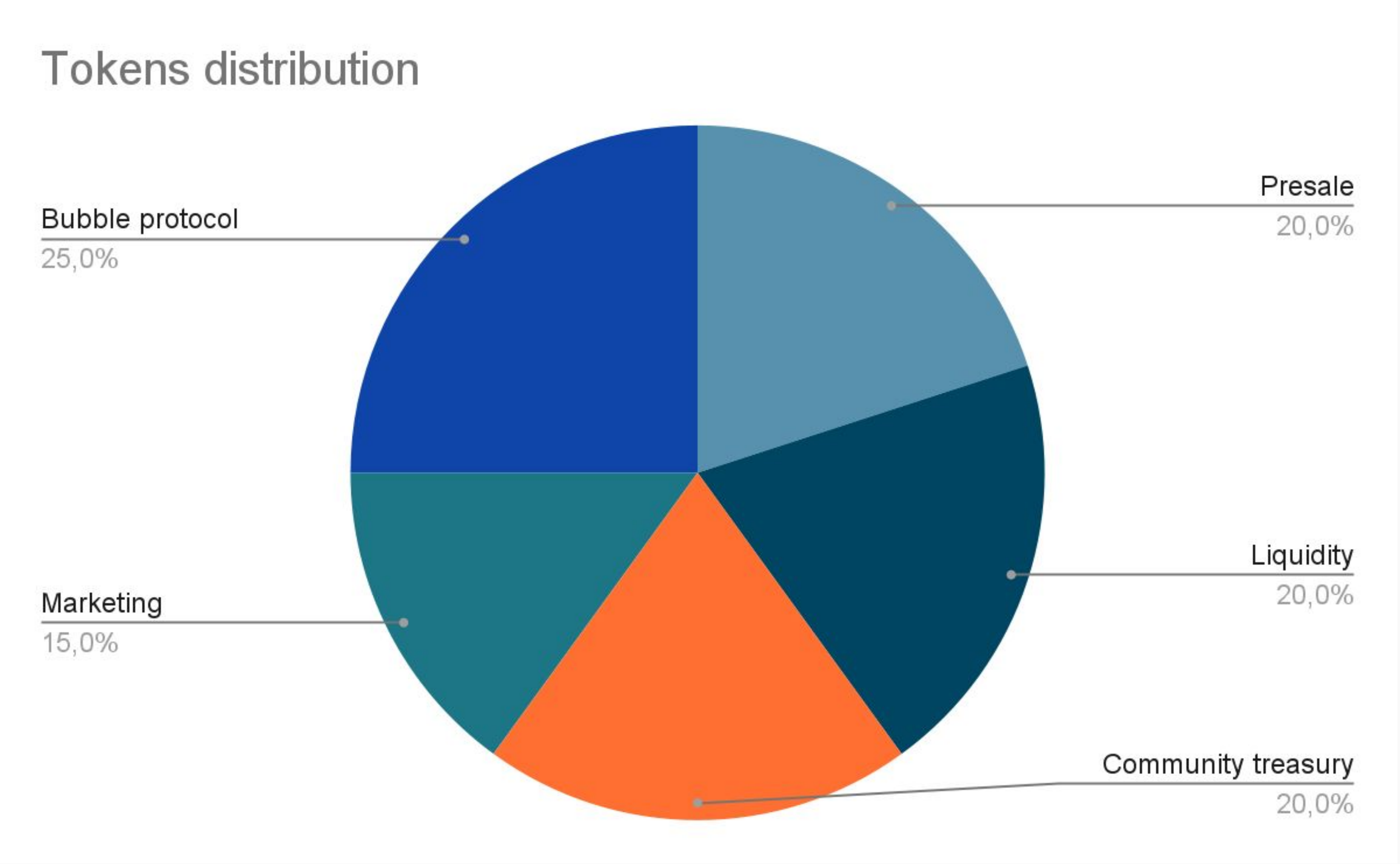
GOOD PRACTICES FOUND

✓ The smart contract utilizes "SafeMath" to prevent overflows

TOKENOMICS

The following initial token's distribution information is based on project's website and/or whitepaper:

- 20% - Presale
- 20% - Liquidity
- 20% - Bubble community treasury
- 15% - Marketing
- 25% - Bubble protocol



WEBSITE

Website URL
https://bubbledefi.com/

Domain Registry
https://www.namecheap.com

Domain Expiration
Expires on 2023-12-04

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

Design
Single page design, appropriate color scheme and graphics.

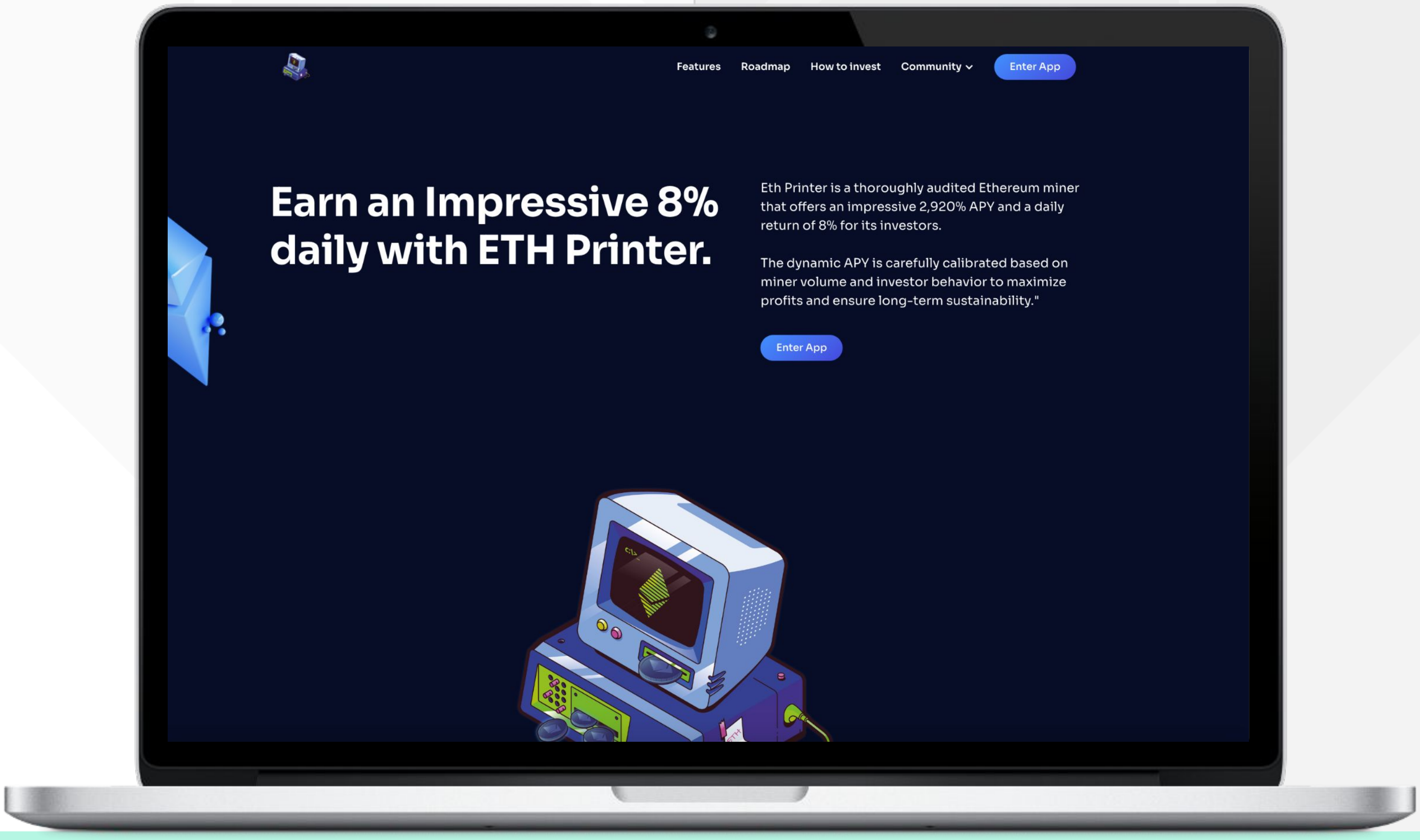
Content
The information helps new investors understand what the product does right away. No grammar mistakes found

.

Whitepaper
Well written, explanatory.

Roadmap
Yes, goals set with time frames.

Mobile-friendly?
Yes



Earn an Impressive 8% daily with ETH Printer.

Eth Printer is a thoroughly audited Ethereum miner that offers an impressive 2,920% APY and a daily return of 8% for its investors.

The dynamic APY is carefully calibrated based on miner volume and investor behavior to maximize profits and ensure long-term sustainability."

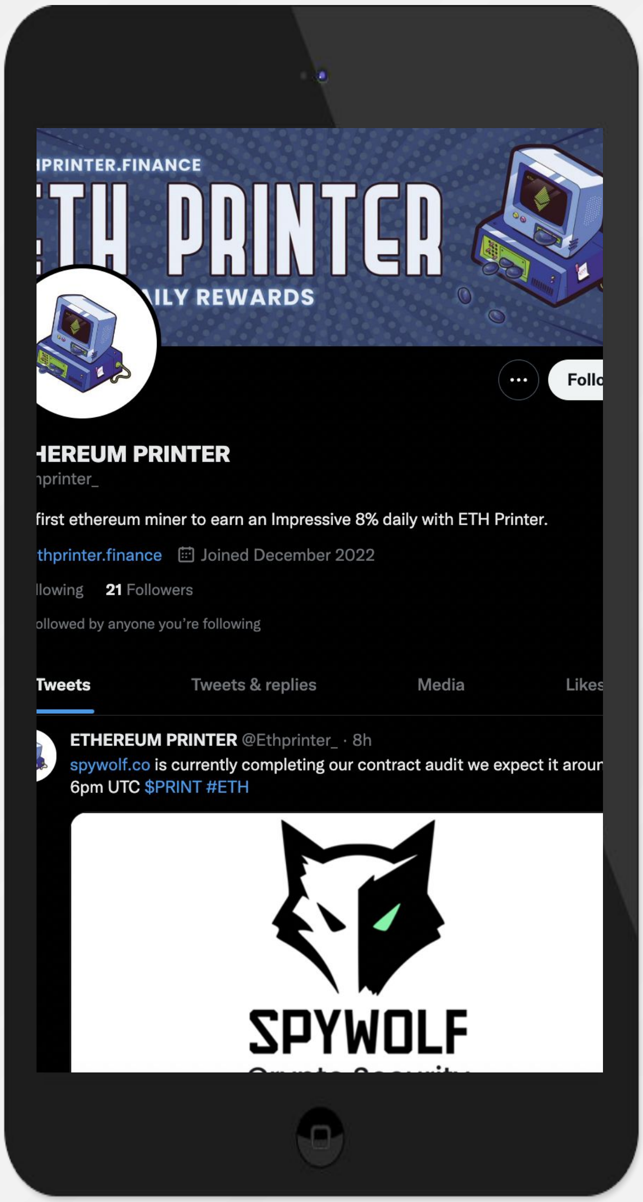
bubbledefi.com

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project's social media pages are active with organic members



HEREUM PRINTER
nprinter_

first ethereum miner to earn an Impressive 8% daily with ETH Printer.

thprinter.finance Joined December 2022

llowing 21 Followers

ollowed by anyone you're following

Tweets Tweets & replies Media Likes

ETHEREUM PRINTER @Ethprinter_ · 8h
spywolf.co is currently completing our contract audit we expect it arour
6pm UTC $PRINT #ETH

Twitter

@Bubble_DeFi

- 1,133 followers
- Active
- Posts frequently

Discord

https://discord.com/invite/KuErdJfkMZ

- 1,474 members
- Active members
- Active mods

Telegram

- Not available

Medium

@Bubble_DeFi

- 73 followers
- 4 articles

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 150 SUCCESSFUL CLIENTS
- ✓ MORE THAN 500 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

SPYWOLF.NETWORK

@SPYWOLFNETWORK

@SPYWOLFOFFICIAL

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.